TLP: WHITE
Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.
http://www.us-cert.gov/tlp/

DATE(S) ISSUED:
01/26/2017

SUBJECT:
Multiple Vulnerabilities in Google Chrome Could Allow for Remote Code Execution

OVERVIEW:
Multiple vulnerabilities have been discovered in Google Chrome, the most severe of which could result in remote code execution. Google Chrome is a web browser used to access the Internet. These vulnerabilities can be exploited if a user visits, or is redirected to, a specially crafted web page. Successful exploitation of these vulnerabilities could allow an attacker to execute remote code in the context of the browser, obtain sensitive information, bypass security restrictions, or cause denial-of-service conditions.

THREAT INTELLIGENCE:
There are currently no reports of these vulnerabilities being exploited in the wild.

SYSTEMS AFFECTED:
- Google Chrome prior to 56.0.2924.76

RISK:
Government:
- Large and medium government entities: **High**
- Small government entities: **Medium**

Businesses:
- Large and medium business entities: **High**
- Small business entities: **Medium**

Home users: Low

TECHNICAL SUMMARY:
Multiple vulnerabilities have been discovered in Google Chrome, the most severe of which could result in remote code execution. These vulnerabilities can be exploited if a user visits, or is redirected to, a specially crafted web page. Details of the vulnerabilities are as follows:

- Multiple cross-site scripting vulnerabilities exist in Blink. (CVE-2017-5006, CVE-2017-5007, CVE-2017-5008, CVE-2017-5010)
- A security bypass vulnerability affects the DevTools. (CVE-2017-5011)

- An unspecified memory-corruption vulnerability occurs due to an out-of-bounds memory access error in the WebRTC. (CVE-2017-5009)
- An unspecified heap corruption vulnerability exists in V8. (CVE-2017-5012)
- Multiple security vulnerabilities exist due to address spoofing in Omnibox. (CVE-2017-5013, CVE-2017-5015)
- An unspecified heap corruption vulnerability exists in Skia. (CVE-2017-5014)
- A security vulnerability exists due to a use-after-free error in Renderer. (CVE-2017-5019)
- A security vulnerability exists due to a UI spoofing in Blink. (CVE-2017-5016)
- An unspecified memory-corruption vulnerability exists due to a memory access error in webm video. (CVE-2017-5017)
- A cross-site scripting exists in 'chrome://apps'. (CVE-2017-5018)
- A cross-site scripting exists in 'chrome://downloads'.(CVE-2017-5020)
- A security vulnerability exists due to a use-after-free error in Extensions. (CVE-2017-5021)
- A security vulnerability exists due to CSP bypass in Blink. (CVE-2017-5022)
- A security vulnerability exists due to a type confusion error in 'metrics'. (CVE-2017-5023)
- Multiple unspecified heap corruption vulnerabilities exist in FFmpeg. (CVE-2017-5024, CVE-2017-5025)
- A security vulnerability exists due to a UI spoofing. (CVE-2017-5026)

Successful exploitation of these vulnerabilities could allow an attacker to execute remote code in the context of the browser, obtain sensitive information, bypass security restrictions, or cause denial-of-service conditions.

RECOMMENDATIONS:
The following actions should be taken:
- Apply appropriate patches provided by Google to vulnerable systems immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from un-trusted sources.
- Apply the Principle of Least Privilege to all systems and services.

REFERENCES:
Google:
https://chromereleases.googleblog.com/2017/01/stable-channel-update-for-desktop.html

CVE:
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5006
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5007
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5008
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5009
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5010
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5011
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5012

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5013
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5014
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5015
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5016
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5017
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5018
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5019
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5020
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5021
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5022
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5023
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5024
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5025
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5026